Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] A transponder-reader transaction system configured with a biometric security system, said system comprising:
a transponder configured to communicate with a reader;
a reader configured to communicate with said system;
a fingerprint sensor configured to detect a proffered fingerprint sample, said fingerprint sensor configured to communicate with said system; and,
a device configured to verify said proffered fingerprint sample to facilitate a transaction.

[c2] The transponder-reader transaction system of claim 1, wherein said sensor is configured to communicate with said system via at least one of a transponder, a reader, and a network.

[c3] The transponder-reader transaction system of claim 1, wherein said fingerprint sensor is configured to facilitate a finite number of scans.

[c4] The transponder-reader transaction system of claim 1, wherein said fingerprint sensor is configured to log at least one of a detected fingerprint sample, processed

fingerprint sample and stored fingerprint sample.

[c5] The transponder-reader transaction system of claim 1, further including a database configured to store at least one data packet, wherein said data packet includes at least one of proffered and registered fingerprint samples, proffered and registered user information, terrorist information, and criminal information.

[c6] The transponder-reader transaction system of claim 5, wherein said database is contained in at least one of the transponder, transponder reader, sensor, remote server, merchant server and transponder-reader system.

[c7] The transponder-reader transaction system of claim 6, wherein said remote database is configured to be operated by an authorized sample receiver.

[c8] The transponder-reader transaction system of claim 1, wherein said fingerprint sensor device is configured with at least one of an optical scanner and capacitance scanner.

[c9] The transponder-reader transaction system of claim 1, wherein said fingerprint sensor device is configured to detect and verify finger print minutia including at least one of ridge endings, bifurcation, lakes, enclosures, short ridges, dots, spurs, crossovers, pore size, pore lo-

cation, loops, whorls, and arches.

[c10] The transponder-reader transaction system of claim 1, wherein said fingerprint sensor device is configured to detect and verify blood flow, correctly aligned ridges, pupil dilation, pressure, motion, and body heat.

[c11] The transponder-reader transaction system of claim 1, further including a device configured to compare a proffered fingerprint sample with a stored fingerprint sample.

[c12] The transponder-reader transaction system of claim 11, wherein said device configured to compare a fingerprint sample is at least one of a third-party security vendor device and protocol/sequence controller.

[c13] The transponder-reader transaction system of claim 11, wherein a stored fingerprint sample comprises a registered fingerprint sample.

[c14] The transponder-reader transaction system of claim 13, wherein said registered fingerprint sample is associated with at least one of: personal information, credit card information, debit card information, savings account information, and loyalty point information.

[c15] The transponder-reader transaction system of claim 14,

wherein different registered fingerprint samples are associated with a different one of: personal information, credit card information, debit card information, savings account information, and loyalty point information.

[c16] The transponder-reader transaction system of claim 14, wherein a fingerprint sample is primarily associated with at least one of first user information, wherein said first information comprises personal information, credit card information, debit card information, savings account information, and loyalty point information, and wherein a fingerprint sample is secondarily associated with at least one of second user information, wherein said second information comprises personal information, credit card information, debit card information, savings account information, and loyalty point information, where second user information is different than first user information.

[c17] The transponder-reader transaction system of claim 1, wherein said transponder-reader transaction system is configured to begin mutual authentication upon verification of said proffered fingerprint sample.

[c18] The transponder-reader transaction system of claim 1, wherein said transponder is configured to deactivate upon rejection of said proffered fingerprint sample.

[c19] The transponder-reader transaction system of claim 1, wherein said sensor is configured to provide a notification upon detection of a sample.

[c20] The transponder-reader transaction system of claim 1, wherein said device configured to verify is configured to facilitate at least one of access, activation of a device, a financial transaction, and a non-financial transaction.

[c21] The transponder-reader transaction system of claim 1, wherein said device configured to verify is configured to facilitate the use of at least one secondary security procedure.

[c22] A method for facilitating biometric security in a transponder-reader transaction system comprising: proffering a fingerprint to a fingerprint sensor communicating with said system to initiate verification of a fingerprint sample for facilitating authorization of a transaction.

[c23] The method for of claim 22, further comprising registering at least one fingerprint sample with an authorized sample receiver.

[c24] The method of claim 23, wherein said step of registering further includes at least one of: contacting said authorized sample receiver, proffering a fingerprint to said

authorized sample receiver, processing said fingerprint to obtain a fingerprint sample, associating said fingerprint sample with user information, verifying said fingerprint sample, and storing said fingerprint sample upon verification.

[c25] The method of claim 22, wherein said step of proffering includes proffering a fingerprint to at least one of an optical and capacitance scanner.

[c26] The method of claim 22, wherein said step of proffering further includes proffering a fingerprint to a fingerprint sensor communicating with said system to initiate at least one of: storing, comparing, and verifying said fingerprint sample.

[c27] The method of claim 22, wherein said step of proffering a fingerprint to a fingerprint sensor communicating with said system to initiate verification further includes processing database information, wherein said database information is contained in at least one of a transponder, transponder reader, sensor, remote server, merchant server and transponder-reader system.

[c28] The method of claim 22, wherein said step of proffering a fingerprint to a fingerprint sensor communicating with said system to initiate verification further includes com-

paring a proffered fingerprint sample with a stored fingerprint sample.

[c29] The method of claim 28, wherein said step of comparing includes comparing a proffered fingerprint sample to a stored fingerprint sample by using at least one of a third-party security vendor device and protocol/sequence controller.

[c30] The method of claim 28, wherein said step of comparing includes comparing fingerprint minutia.

[c31] The method of claim 30, wherein said step of comparing minutia comprises storing, processing and comparing at least one of ridge endings, bifurcation, lakes, enclosures, short ridges, dots, spurs, crossovers, pore size, pore location, loops, whorls, and arches.

[c32] The method of claim 22, wherein said step of proffering a fingerprint to a fingerprint sensor communicating with said system further comprises using said fingerprint sensor to detect at least one of blood flow, correctly aligned ridges, pupil dilation, pressure, motion, and body heat.

[c33] The method of claim 22, wherein said step of proffering a fingerprint to a fingerprint sensor communicating with said system to initiate verification further includes at

least one of detecting, processing and storing at least one second proffered fingerprint sample.

[c34] The method of claim 22, wherein said step of proffering a fingerprint to a fingerprint sensor communicating with said system to initiate verification further includes the use of at least one secondary security procedure.

[c35] A method for facilitating biometric security in a transponder-reader transaction system comprising:
detecting a proffered fingerprint at a sensor communicating with said system to obtain a proffered fingerprint sample;
verifying the proffered fingerprint sample; and
authorizing a transaction to proceed upon verification of the proffered fingerprint sample.

[c36] The method of claim 35, wherein said step of detecting further includes detecting a proffered fingerprint at a sensor configured to communicate with said system via at least one of a transponder, reader, and network.

[c37] The method of claim 35, wherein said step of detecting a proffered fingerprint includes detecting a proffered fingerprint at one of a capacitance and optical scanner.

[c38] The method of claim 35, wherein said step of detecting includes at least one of: detecting, storing, and process-

ing a proffered fingerprint sample.

[c39] The method of claim 35, wherein said step of detecting further includes receiving a finite number of proffered fingerprint samples during a transaction.

[c40] The method of claim 35, wherein said step of detecting further includes logging each proffered fingerprint sample.

[c41] The method of claim 35, wherein said step of detecting further includes at least one of detection, processing and storing at least one second proffered fingerprint sample.

[c42] The method of claim 35, wherein said step of detecting further includes using said fingerprint sensor to detect at least one of blood flow, correctly aligned ridges, pupil dilation, pressure, motion, and body heat.

[c43] The method of claim 35, wherein said step of verifying includes comparing a proffered fingerprint sample with a stored fingerprint sample.

[c44] The method of claim 43, wherein said step of comparing a proffered fingerprint sample with a stored fingerprint sample comprises storing, processing and comparing at least one of fingerprint minutia.

[c45] The method of claim 43, wherein comparing a proffered

fingerprint sample with a stored fingerprint sample includes comparing a proffered fingerprint sample with at least one of a biometric sample of a criminal, a terrorist, and a transponder user.

[c46] The method of claim 35, wherein said step of verifying includes verifying a proffered fingerprint sample using information contained on at least one of a local database, a remote database, and a third-party controlled database.

[c47] The method of claim 35, wherein said step of verifying includes verifying a proffered fingerprint sample using one of a protocol/sequence controller and a third-party security vendor.